PRIVACY FIRST

your choice in a free society

Annual Report 2018

Privacy First Foundation
Amsterdam

9 December 2019

Table of contents

1. Introduction

In the past year, many developments have taken place with respect to the rule of law and the privacy of citizens has further declined. Developments in the financial world with regard to the *war on cash*, PSD2 and UBO further constrain citizens in their spending sovereignty. In the medical world, centralization and the national Electronic Health Record keep reappearing, while good decentralized alternatives are becoming increasingly available. In general, the 'dragnet philosophy' is leading within government and services, which will put the entire life of citizens under continuous and permanent monitoring. Freedom is traded in for coercion and uniformity to move, think and act within "the norm", based on a large dose of self-censorship. In public spaces, within schools, libraries and shops, the same trend, often stimulated by government and business, can be observed everywhere. This includes the reversal of traditional legal principles. Exceptions become the rule instead of confirming the rule. Privacy First stands for private choices in a free society and, despite the developments mentioned, sees great opportunities for the Netherlands as a pioneer nation in privacy. The highlight of this is the presentation of our annual Dutch Privacy Awards, where companies and organizations introduce sustainable privacy solutions and thus present a shining alternative to the current trend. We will continue many of our actions, court cases and lobbying again in the coming year. In this we hope for your support as a donor!

To a free 2020!

Bas Filippini,
Privacy First chairman

2. Vision and policy

Privacy First was founded in 2008 as an independent foundation to preserve and promote everyone's right to privacy. Privacy is a universal human right and the basis of our democratic constitutional State. In addition to the right to a private life, the right to privacy also includes the protection of personal data, confidential communication and physical integrity. Of all human rights, the right to privacy is currently under most pressure. Privacy First is therefore committed to protecting and promoting this right as much as possible. As an Institution of Public Benefit (ANBI), Privacy First does this in the public interest, either for the population as a whole or for vulnerable subgroups. Privacy First uses a broad, fundamental orientation on privacy, both in relation to our free, open society and with regard to other relevant human rights. Our field of vision and our activities extend to both the digital and the analogue domain. However, these worlds are becoming increasingly integrated and ever shrink the classic "analogue space". The impact that technology has on someone's privacy seems to be accelerating. In 2017, terms such as 'Big Data' and 'Cloud' were still buzzwords, now almost every government and business initiative contains terms such as 'smart' and 'artificial intelligence'. Due to a lack of standards and ethical discussion there is a great risk that the Netherlands will become one large 'Living Lab', i.e. in a continuous experimental state without adequate guarantees. To reverse these developments and steer them in the right direction, Privacy First has been advocating *privacy by design* for years: incorporating privacy into services and technology from the very first design phase. The arrival of the new European privacy law GDPR supports us in this ambition. At the same time, Privacy First operates in a force field that constantly threatens privacy. The work of Privacy First is therefore becoming increasingly urgent and relevant.

Privacy First's consistent policy is to focus our attention primarily on (imminent) privacy violations that can affect large groups of people at the same time. In our selection of topics we are guided by 1) the scale, 2) the severity and 3) the impact and consequences of a given violation. Massive, serious privacy violations are first investigated by Privacy First and publicly named. Privacy First then attempts to remedy the violation in question by means of silent diplomacy and political lobbying, followed by a public campaign, legal action or - as a last resort - a lawsuit. In line with these criteria, Privacy First's attention in recent years has focused primarily on biometrics, camera surveillance, public transport chip cards, medical privacy, mobility and anonymity in public spaces. In addition, Privacy First is becoming increasingly active on the theme of privacy & secret services, Big Data, *profiling* and financial privacy.

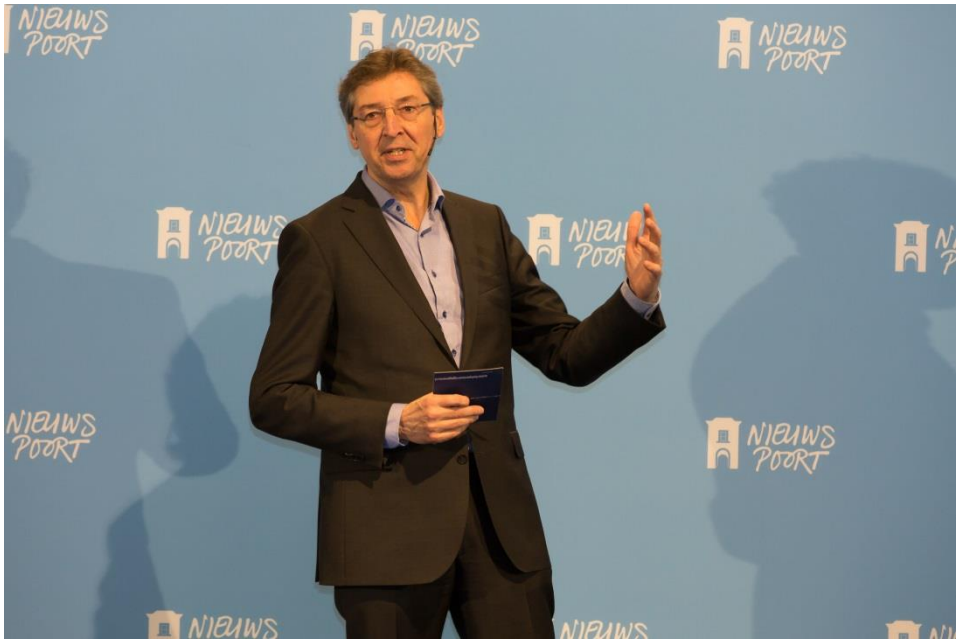
Our core mission is to protect the population from mass surveillance and to develop the Netherlands into an international Pioneer Nation in Privacy. We are happy to describe our main activities from 2018 below.

3. Project and events

3.1 Dutch Privacy Awards and National Privacy Conference

On January 28, 2019, ECP and Privacy First again jointly organized our annual National Privacy Conference. This is now the main annual Dutch privacy event around the European Day of Privacy. Our goal of this event is to work together with the business community, government,

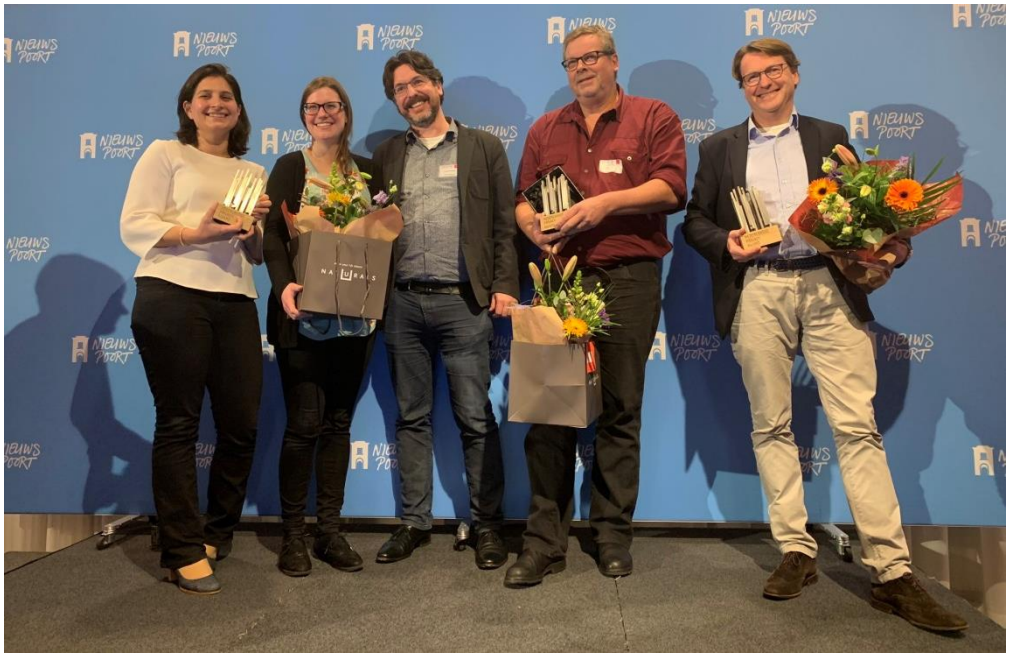
science and civil society to build a privacy-friendly information society and to help develop the Netherlands into an international Pioneer Nation in Privacy. This time the conference location was Nieuwspoort in The Hague and the interest again turned out to be huge: more than 200 professionals had registered for free, with a room capacity of 160 people. Every conference participant received the "The Little Blue Book" by Dr. Jaap-Henk Hoepman (Radboud University Nijmegen) about *privacy by design*. Keynote speakers during the conference were Aleid Wolfsen (Data Protection Authority), Sophie in 't Veld (European Parliament), Brenno de Winter, Jeroen Terstegge (Privacy Management Partners) and Tijmen Schep (Setup). Chairman of the day was presenter Tom Jessen (RTL, BNR).



Aleid Wolfsen (Dutch Data Protection Authority chairman) during the National Privacy Conference, 28 January 2019. Photo: Tamara Heck.

As a concluding part of the conference, Privacy First presented our annual Dutch Privacy Awards. In the summer of 2018, Privacy First itself (at its own expense and with its own staff) developed a special website for the Awards: www.privacyawards.nl. Subsequently, Privacy First received nearly 20 entries for the Awards, most of which were of very high quality. Evaluation of all entries and company visits by our independent Awards Jury then took place during the fall and winter of 2018. Nominated in the Consumer Solutions category were *Private Search 2.0* (Startpage.com), *VraagApp* and *Schluss*, in the Business Solutions category *Privacy op Schooltas* and *Privacy Designer* (Privacy Company & SURF) and in the Public services category *Passantentellingen* (municipality of Nijmegen) and the *Privacy by Design* project of the Dutch Tax Authorities. During the conference, all nominees presented their projects to the public through Award pitches. Private Search 2.0 and Privacy Designer were then named winners by the jury. In addition, the Encouragement Prize went to the PublicSpaces initiative.

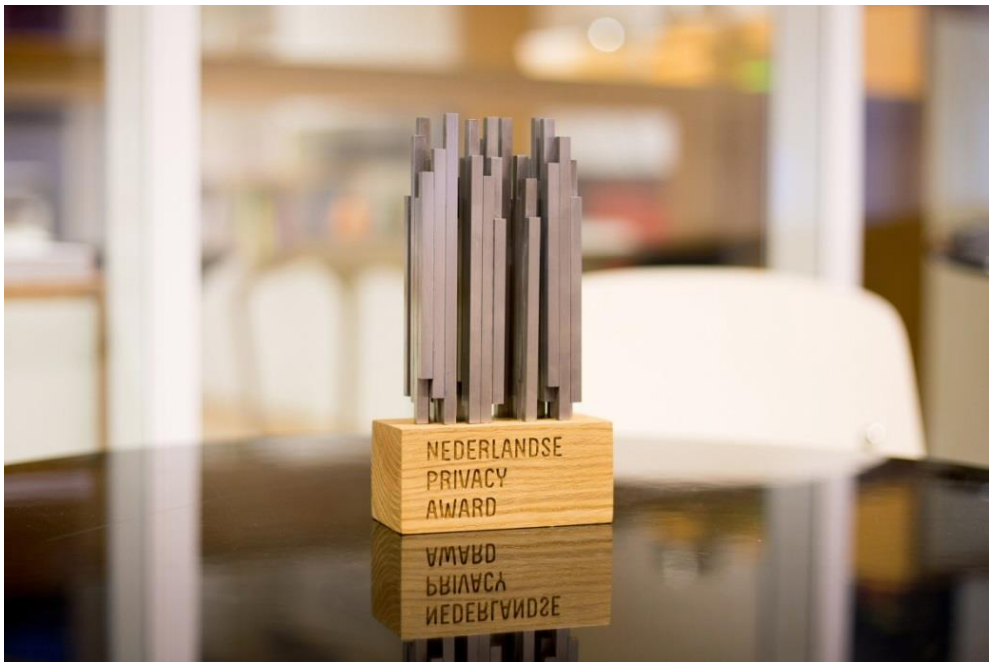
Nederlandse PRIVACY AWARDS



Winners of the Dutch Privacy Awards 2019.

The jury of the Dutch Privacy Awards in 2018 consisted of the following people:
- Bart van der Sloot (senior researcher, Tilburg University; jury chairman)
- Bas Filippini (founder and chairman of Privacy First)
- Paul Korremans (partner Comfort-IA; data protection officer; member of the Privacy First board)
- Marie-José Bonthuis (owner IT's Privacy)
- Esther Janssen (lawyer in Information law and fundamental rights, Bureau Brandeis)
- Esther Keymolen (technology philosopher, Tilburg University)
- Matthijs Koot (senior security specialist, Secura BV)
- Marc van Lieshout (senior researcher TNO and business director PI.lab)
- Wendeline Sjouwerman (privacy specialist for local governments and healthcare).

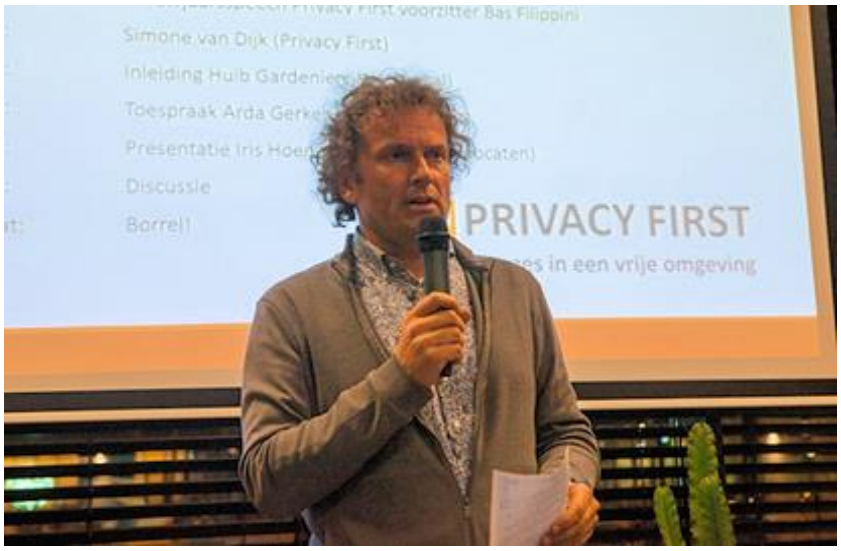
You can find a detailed report (in Dutch) of the congress and the Awards on our website.



The National Privacy Conference and the Dutch Privacy Awards were made possible in 2018 with the help of the Democracy & Media Foundation. At the beginning of 2020, Privacy First and ECP will again organize this inspiring event. Would your organization like to become a partner or sponsor? Then contact Privacy First!

3.2 Public debate about children and privacy

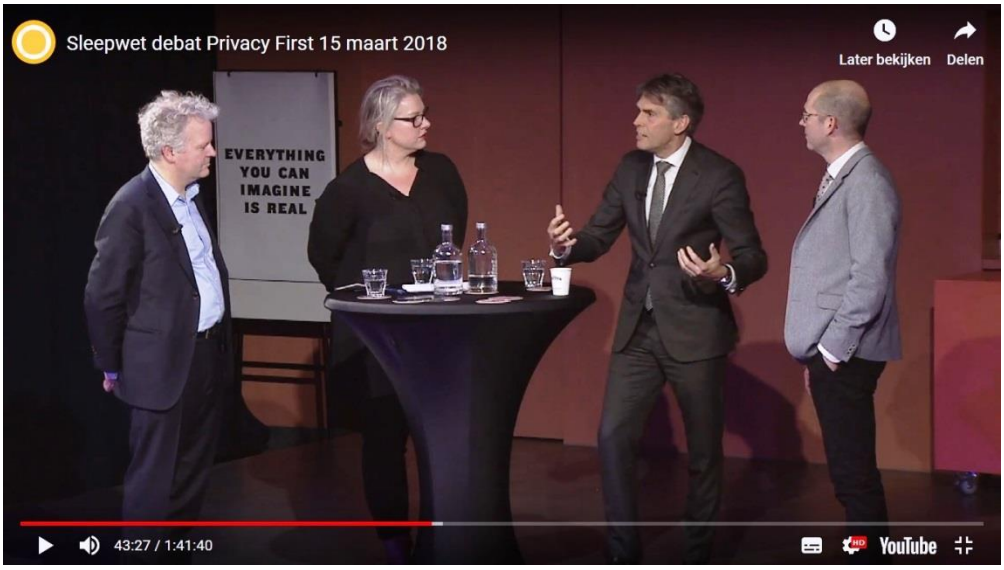
At the beginning of 2018, Privacy First organized a well-attended New Year's reception and successful public debate on the theme of children & privacy at our office location in the Volkshotel (Amsterdam). Speakers were Bas Filippini (Privacy First), Huib Gardeniers (Net2Legal), Simone van Dijk (Privacy First), Arda Gerkens (Senate) and Iris Hoen (Wille Donker Attorneys). For an extensive report, see https://www.privacyfirst.nl/solutions/evenementen/item/1103-verslag-van-publieksdebat-over-kinderen-privacy.html. Privacy First has growing concerns in this area and has been increasingly active since 2018 to promote the privacy of children and pupils (especially in primary education), primarily through critical discussions with responsible organizations in the private and public sector.



New Year's speech by Bas Filippini (Privacy First chairman), 17 January 2018. Photo: Bertus Gerssen.

3.3 Debate on 'Dragnet Act' referendum

In the context of the Dutch national referendum on the new Intelligence and Security Services Act, Privacy First organized a critical public debate on 15 March 2018 in the Parool Theatre (Amsterdam) on the privacy aspects of this new 'Dragnet Act'. The entire debate evening was broadcast live on the internet and, in the run-up to the referendum, also fully repeated several times on national television by NPO Politiek. Speakers during this evening were Dick Schoof (National Coordinator for Counterterrorism and Security), Nine de Vries (Amnesty International Netherlands) and Otto Volgenant (Boekx Attorneys). Our moderator was Bart de Koning (investigative journalist in the field of privacy and security). During the debate there was a lot of room for discussion between the speakers themselves and with the audience, followed by drinks where we could toast together to a successful referendum!

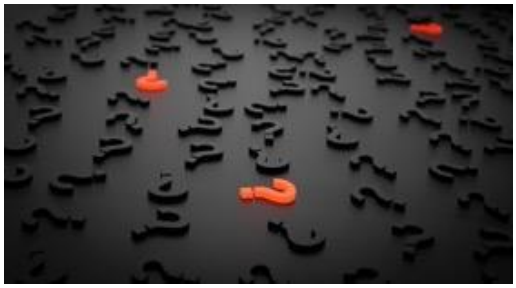


Debate on 'Dragnet Act' referendum, 15 March 2018. Left to right: Bart de Koning, Nine de Vries, Dick Schoof and Otto Volgenant. Picture: Engage TV.

3.4 Privacy First Solutions

Privacy First is increasingly being asked for advice by companies and governments. In exceptional cases, when the intentions of the organization concerned are in line with the mission of Privacy First, we happily make our contribution. Privacy First has been doing this for several years under the banner of our umbrella project Privacy First Solutions. Examples of Privacy First Solutions projects in 2018 were the development of a possible quality label concerning the new European payment directive PSD2 together with the Volksbank and the Dutch Payments Association. In this context, Privacy First also took the initiative at the end of 2018 for the development of a do-not-PSD2-me-register, see our new bi-lingual campaign website www.psd2meniet.nl. In addition, Privacy First (at the initiative of the Dutch Tax Authorities) has been critically involved since October 2018 in a High Pressure Privacy Impact Assessment (DPIA) within the Tax Authorities, carried out externally by Privacy Management Partners (PMP). In this way Privacy First tries - in the public interest - to positively influence certain societal developments and to ensure that privacy is safeguarded as much as possible not only "from the outside" but also "from the inside". Privacy First expects to be able to initiate various other Solutions projects with new partners in 2019.

3.5 Privacy First as a daily information desk



Privacy First is approached daily through telephone and email by citizens, journalists and students with a wide range of questions and requests in the field of privacy. Privacy First always tries to answer these questions as well and as quickly as possible, but this requires (sometimes too) much from our small foundation. For this reason, Privacy First sometimes refers people to other relevant organizations, agencies, legal experts and lawyers.

3.6 Interns

In 2018, a law student successfully wrote her thesis at Privacy First on the ANPR Bill. New interns and thesis students are always welcome at Privacy First, if currently relevant to our field of work.

3.7 Other activities

In 2018, Privacy First was active at various relevant conferences, seminars and meetings, including at Leiden University, Platform for the Protection of Civil Rights, Housing Union, ECP, Institute for Information Law (UvA), Amnesty International, Volksbank, the Royal Library, NJCM, University of Amsterdam (speaker), Nieuwspoort, KPMG, Committee of Vigilance, Pro Bono Connect, Privacy Law Association, Pirate Party, CTIVD, V@School, Humanist Association, Vitens, WODC, Tilburg University, VVD (speaker), Parliamentary System State Committee, Hague Internet Summit (UN, Peace Palace), Facebook, Tax Authorities, Ministry of Justice and Security (speaker), Fox IT, Kaspersky, PILP, DNB (speaker), Good Pitch Europe, Lions (speaker), Municipality of Haarlem, National Institute for Human Rights, National Referendum Committee, Privacy Management Partners, One Conference, Dutch Data Protection Authority, Association of Ethics, Dutch Payments Association, IIR (speaker), National Ombudsman, Association for Biometrics & Identity (speaker) and Waag Society.

Privacy First's employees are regularly invited as speakers at public events of government, business and science. In that context, Privacy First has been working with the Athenas speaker agency for several years. Furthermore, Privacy First continuously conducts silent diplomacy in our broad field of work; in this context, Privacy First had numerous meetings with governments, companies and other organizations in 2018.

4. Political lobbying

4.1 Dragnet Act referendum campaign

The most important and influential activity of Privacy First in 2018 was our campaign in the run-up to the referendum on the new Dutch Act on Intelligence and Security Services, the so-called Dragnet Act. As one of the first organizations in the Netherlands, Privacy First received a relatively high subsidy for this from the National Referendum Committee. Privacy First subsequently spent these funds on various Dragnet Act campaign activities in the period January - March 2018, consisting of 1) a critical public debate, 2) campaign on the Privacy First website, 3) activation of media and influencing public opinion, 4) news monitoring and campaign on social media, 5) press advertisements and 6) political lobbying and silent diplomacy.

A large part of the population was reached by these activities, and with success: on March 21, 2018, a narrow majority voted AGAINST the Dragnet Act. In addition to this success, our campaign has probably also led to higher national privacy awareness in general. Following the referendum, there was also a promise from the government of a limited use of the new dragnet power in the domestic domain. Moreover, the referendum has generated political pressure to critically revise the Dragnet Act. Nevertheless, the Dragnet Act entered into force virtually unchanged on 1 May 2018 and the promised legislative changes still have not been submitted.

4.2 New law on organ donation

In February 2018, the Dutch Senate passed a controversial new law on organ donation by a narrow majority. Unless an active objection is made (or has already been made), every Dutch person will be automatically registered as an organ donor. Privacy First had strongly advised the Senate in advance to vote against this law, since in our view it violates the right to privacy and physical integrity. The right to physical integrity is part of the right to privacy and is protected as such under both art. 8 ECHR and art. 11 of the Dutch Constitution. Art. 11 of the Constitution also applies after death. Moreover, unlike some other privacy rights, the right to physical integrity and physical self-determination has a relatively absolute character; in principle, everyone has prior explicit control of his/her own body and organs. Only with explicit and specific (organ-differentiated) individual permission in advance can a person be registered as an organ donor. A donor system whereby everyone is declared a donor in advance by the government is by definition contrary to this. Privacy First therefore regrets that a law as far-reaching as this Donor Act, which is so divisive and lacks broad public support, has been passed by the Senate.

4.3 EU Passenger Name Records (PNR)

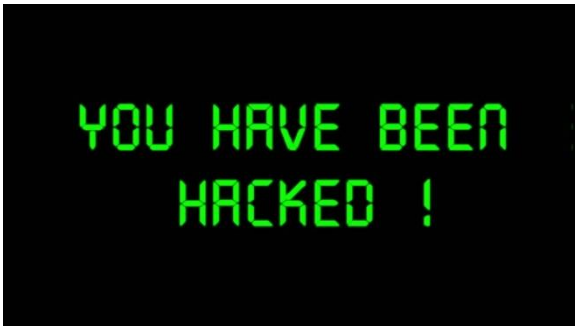
After years of delay (due to privacy concerns), in 2018 the Dutch implementation of the EU Passenger Name Records (PNR) Directive was discussed in Parliament. Despite structural criticism from Privacy First, the Dutch PNR Act was subsequently adopted by both Parliament and the Senate. Because of this new PNR law, countless data of all air passengers with departure or arrival in the Netherlands will be kept for 5 years in a central government database and used for the prevention, detection, investigation and prosecution of crimes and terrorism. Sensitive personal data (including name and address data, telephone numbers, email addresses, birth dates, travel dates, ID document numbers, destinations, fellow passengers and payment data) of many millions of passengers will therefore be available for years for data mining and profiling purposes. This amounts to mass surveillance of mostly innocent civilians.

To this day, the legally required societal necessity and proportionality of this system has not been demonstrated. PNR thus constitutes a blatant violation of the right to privacy and freedom of movement. Moreover, the effectiveness of PNR has never been demonstrated to date: "statistical evidence is not available," said the responsible Dutch Minister for Justice and Security, Grapperhaus. Privacy First therefore expects that the EU PNR Directive will soon be reviewed by the European Court of Justice and declared illegal. After that, the same situation will arise as a few years ago with regard to EU telecom data retention: as soon as this European directive has

been declared invalid, the Dutch implementation legislation will be abolished by Privacy First in summary proceedings.

4.4 Bill on Computer Crime III ("police hacking law")

In June 2018, the Dutch Senate adopted the controversial Bill on Computer Crime III. This law gives the police the authority to hack almost any device. However, this law has never had a thorough and independent Privacy Impact Assessment. The required social necessity and proportionality of this law have not been demonstrated to date either. In Privacy First's view, this type of legislation is mainly driven by technological determinism: everything that is technically possible is made legally possible. There is by design no question of any legal curtailment in the technological sense: the effect of the Bill will extend to almost everything that is connected to the internet. In the future, therefore, this will include almost all of society, including the Internet of Things. Some within the police even want to be able to hack and stop moving cars, with all associated dangers for road safety. Moreover, the crimes for which this Bill can be deployed can simply be extended by the Minister through General Administrative Order. Privacy First has therefore asked Parliament several times to reject this law, or at least to restrict it. Partly as a result of our criticism, the deployment of the new powers will be reviewed in advance by an examining magistrate and there will be no hacking of innocent third parties.



4.5 Abolition of consultative referendum

Despite the successful referendum on the new Intelligence and Security Services Act, the Dutch Senate abolished the consultative referendum in June 2018. Privacy First regrets this and expects that this will further widen the existing gap between citizens and government. It will also lead to a further loss of confidence in national politics. This weakens our democracy and, without the corrective effect of the referendum, also our rule of law.

In international law, a national referendum is a form of internal self-determination: the collective right of a national population to determine its own democratic future. Like all human rights, this right must be constantly protected and promoted. Moreover, a referendum is a democratic achievement that cannot simply be abolished without legitimate cause and objective justification. This is possibly in violation of the prohibition of regression of human rights: the international prohibition of simply reversing democratically acquired rights of citizens. At the beginning of 2018, Privacy First made the Senate and Parliament aware of this in vain. As a result, the Senate invited Privacy First in March 2018 for an expert meeting on the international legal aspects of the consultative referendum. Afterwards, Privacy First also raised the Dutch abolition of the referendum at the United Nations and had the Dutch government held accountable for this at the UN Human Rights Committee in Geneva.

Apart from former East-Germany, the Netherlands is now the only country in the world that has abolished the referendum after its introduction. After Athens (democracy 1.0) and our current 19th-century parliamentary democracy (2.0), in the view of Privacy First, it is therefore high time for more citizen participation and democratic renewal: *Shared Democracy*, democracy 3.0. Like the Dutch Parliamentary System State Committee, Privacy First advocates the introduction of a binding corrective referendum (and a Constitutional Court) to strengthen our democratic constitutional State. Privacy First will remain committed to these goals.

4.6 Introduction of Taser weapons in the police force

In 2018, the Dutch section of the International Commission of Jurists (NJCM) sent a so-called "shadow report" on behalf of a broad coalition of civil society organizations about the Netherlands to the UN Committee against Torture. On the initiative of Privacy First, the issue of Taser weapons was, just like in 2013, explicitly raised in this report. The Dutch government has been planning for years to give every Dutch police officer their own Taser weapon. To date, only the Dutch police's arrest teams have been equipped with Taser weapons. It is expected that a broader, general use of Taser weapons will lead to structural excesses. In this context, Taser weapon scandals in the U.S. in particular are very notable. In Privacy First's view, the use of Taser weapons can easily lead to a violation of the international ban on torture, cruel or inhuman treatment and the related right to physical integrity. Taser weapons lower the violence threshold and hardly leave any external traces. At the same time, Taser weapons can cause serious physical and mental damage. This poses serious risks for the Dutch population, especially for certain vulnerable groups.

Partly as a result of the critical input from Privacy First, the UN Committee against Torture issued a number of guidelines (*Concluding Observations*) to the Dutch government in December 2018, including the urgent request not to introduce Taser weapons for the entire Dutch police force and limit them to those cases where the use of a Taser weapon can be deemed strictly necessary and proportionate. The Committee also expressly warns against the use of Taser weapons with vulnerable people. In addition, the Committee is very concerned about the way Taser weapons have been used by the Dutch police so far. Privacy First appreciates this critical view and the principled position of the Committee. This also creates a strong precedent for other countries worldwide. Privacy First will continue to ensure that the Dutch government complies with the guidelines of the Committee.

4.7 Mandatory fingerprints in identity cards

Since 2009 in the Netherlands, the controversial EU obligation to include fingerprints in passports has been in force. Until now, identity cards have been excluded from this European obligation. Nevertheless, since 2009, fingerprints have also been included in Dutch identity cards. Due to privacy concerns, this Dutch obligation was abolished in January 2014 and was declared unlawful

by the Dutch Council of State *(Raad van State)* in 2016 with retroactive effect. Since then, however, the European Commission has been working on new European legislation to make it compulsory to include fingerprints in all European identity cards. Privacy First has called on the Dutch government several times to oppose this. After all:

1. In May 2016, the Council of State already ruled that the mandatory inclusion of fingerprints in Dutch identity cards violates the right to privacy due to lack of necessity and proportionality.

2. Various freedom of information requests from Privacy First in recent years have shown that the issue to be tackled (look-alike fraud with ID documents) is of such a small scale that mandatory fingerprinting to combat it is completely disproportionate and therefore unlawful.

3. Fingerprints in passports and ID cards have been subject to a biometric error rate of no less than 30% in recent years, Dutch Deputy Minister Teeven acknowledged in Parliament. Minister Donner previously admitted an error rate of 21-25% in Parliament.

4. Partly due to these high error rates, fingerprints in passports and identity cards are virtually unused to date. At national borders, at customs and at airports, fingerprints are not even used at all.

5. Due to the high error rates, Deputy Minister Bijleveld (Home Affairs) already instructed all Dutch municipalities in September 2009 not to perform fingerprint verifications when issuing passports and identity cards. In the case of a biometric “mismatch”, after all, the relevant ID document must be returned to the passport manufacturer, which in high numbers would lead to rapid societal disruption. The Ministry of the Interior was concerned in this context about social unrest and even possible violence at municipal counters. The relevant concerns and instructions from the Ministry of the Interior still apply to date.

6. Various individual Dutch legal cases are still pending before the European Court of Human Rights in which the mandatory issue of fingerprints for passports and ID cards is being challenged due to violation of art. 8 ECHR (right to privacy).

7. For people who for whatever reason do not wish to give fingerprints (biometric conscientious objectors, art. 9 ECHR) an exception should be stipulated in any case.

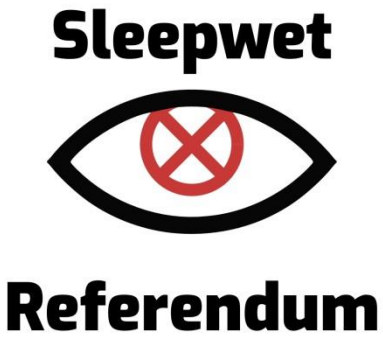
5. Court cases

As a civil society organization, Privacy First aims to operate as effectively as possible with the limited resources that we have. If silent diplomacy, political lobbying and campaigns prove fruitless, Privacy First therefore conducts fundamental lawsuits against legislation and policy that lead to large-scale privacy violations. In recent years Privacy First has successfully done this against the central storage of everyone's fingerprints under the Dutch Passport Act and the storage of everyone's telecommunications data under the Telecommunications Data Retention

Act. Privacy First prefers to conduct such matters in a coalition, and through pro bono support by suitable law firms.

5.1 New Intelligence and Security Services Act ('Dragnet Act')

In July 2017, the Dutch Senate passed the controversial new Intelligence and Security Services Act. As a result of this law, mass surveillance in the Netherlands is now on the verge of becoming a *fait accompli*: new powers under this law include a massive internet tap that allows large groups of people to be intercepted at the same time. To prevent this, a national referendum on this so-called "Dragnet Act" took place on March 21, 2018, at the initiative of five students from Amsterdam. During this referendum, a majority of the Dutch population clearly opposed this law. In response to this, however, the Dutch government has only announced a few brief, superficial policy changes and some non-fundamental legislative changes. The "Dragnet Act" subsequently entered into force virtually unchanged on 1 May 2018.



Summary proceedings against Dragnet Act

Privacy First's consistent policy is to prevent massive privacy violations. The entry into force of the current Dragnet Act is unmistakably a massive privacy violation: under this Act, the internet traffic of innocent citizens can be tapped on a large scale. Moreover, these unevaluated data of innocent citizens will be exchanged massively with foreign secret services. This constitutes a blatant violation of the right to privacy. Possible legislative changes to "fix" this afterwards could therefore not be awaited; after all, the privacy violations would have already occurred. A broad coalition of, among others, Bits of Freedom and Privacy First therefore requested the government in April 2018 to postpone the introduction of (the most privacy-violating parts of) the Dragnet Act until all the desired legislative changes had been debated in Parliament. After the government refused this request, our coalition was then forced to conduct summary civil proceedings to have the most privacy-violating parts of the Dragnet Act declared inoperative due to conflict with higher (European) privacy legislation. In addition to Privacy First, the coalition for this summary proceedings consisted of Bits of Freedom, the Dutch section of the International Commission of Jurists (NJCM), Dutch Association of Criminal Lawyers (NVSA), Platform for the Protection of Civil Rights, Free Press Unlimited, BIT, Voys, Speakup, Greenpeace International, Waag Society and Mijndomein Hosting. The case was handled by Boekx Attorneys and coordinated by the Public Interest Litigation Project (PILP) of NJCM. On 7 June 2018 the summary proceedings took place at the district court in The Hague. Unfortunately, the court rejected the case on 26 June 2018. This judgment is extremely disappointing. It is true that the legal bar in this case was high: in order to win these summary proceedings, the court had to declare the Dragnet Act "unmistakably non-binding" due to obvious (unmistakable) conflict with international or European law. The verdict of the judge, however, mainly reads as directed reasoning in favor of the State, in which various objections from our coalition have remained unmentioned. It should

however be emphasized (as the court itself does) that this judgment only involves a preliminary judgment and that there was no question of a thorough, "full" review in this case.

The coalition believes that, partly in view of the outcome of the referendum, the Dutch government should have waited to introduce the challenged sections of the Dragnet Act until the parliamentary legislative process following the referendum was completed. The introduction of the unchanged Dragnet Act on 1 May 2018 and only later (at an unknown future date) submitting improvements to the law is and will remain the incorrect way to proceed.

The coalition has discussed various possible further legal steps. Partly depending on the further parliamentary process, large-scale substantive proceedings against the Dragnet Act are now an option.

5.2 Citizens versus Plasterk case

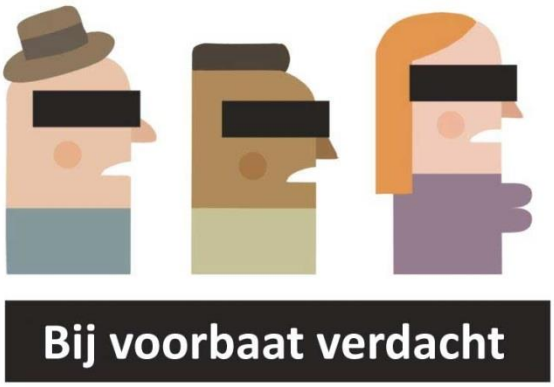
Since the end of 2013, Privacy First has been conducting the "Citizens versus (Minister) Plasterk" case together with other organizations and citizens. The reason for this civil case against the Dutch State was the revelations of Edward Snowden about the practices of (foreign) intelligence services, including the American NSA and British GCHQ. Our coalition demands the State to stop using foreign intelligence that has not been obtained in accordance with Dutch law. Our lawyers at Bureau Brandeis conduct this case from their own pro bono fund for social litigation. The affiliated organizations are: Privacy First, the Dutch Association of Criminal Lawyers (NVSA), the Dutch Association of Journalists (NVJ) and Internet Society Netherlands. However, after negative verdicts from both the district court and the Appeals Court of The Hague, the Dutch Supreme Court also rejected our final appeal in this case on 7 September 2018. The Supreme Court has thus offered a permit for Dutch secret services to continue collecting large amounts of data from Dutch citizens through foreign intelligence services without legal protection. Our lawyers continued this case at the beginning of 2019 at the European Court of Human Rights (ECHR) in Strasbourg. At the same time, a similar case of Big Brother Watch against the British government is pending at the ECHR. Privacy First hopes that the Court will soon reach a critical verdict in both cases.

5.3 System Risk Indication (SyRI)

At the end of March 2018, a broad coalition of civil society organizations summoned the Dutch State to take Systeem Risico Indicatie out of operation. Systeem Risico Indicatie (System Risk Indication, SyRI) uses secret algorithms to screen large groups of people (and even entire residential areas) to secretly profile citizens on their risk of fraud with social services. In addition to the massive violation of the right to privacy, this system also violates the right to a fair trial and has a discriminatory and stigmatizing effect. According to the coalition of plaintiffs, SyRI therefore poses a threat to the rule of law and the legislation on which SyRI is based must be declared unlawful.

The group of plaintiffs consists of the Civil Rights Platform Foundation, Dutch section of the International Commission of Jurists (NJCM), Privacy First, KDVP Foundation, the National Client Council and FNV. Authors Tommy Wieringa and Maxim Februari, who previously expressed very critical opinions about SyRI, have joined the proceedings in their personal capacity. The coalition

is represented by Anton Ekker (Ekker Legal) and Douwe Linders (SOLV Attorneys). This case is also coordinated by the Public Interest Litigation Project (PILP) of the NJCM.



The parties to these proceeding are not opposed to the government combating fraud. They just think that this should happen on the basis of concrete suspicions. Dragnet searches should not be used to look into the private life of non-suspect Dutch citizens for possible fraud risks. According to the claimants, this disproportionate method does more harm than good. There are better and less radical forms of fraud prevention than SyRI.

Fearing this lawsuit, several municipalities (including Rotterdam) have already stopped using SyRI. The court hearing in the case took place on October 29, 2019. The court's verdict is currently planned for 5 February 2020.

For more information and updates, Privacy First refers you to the special campaign website of the Dutch Platform for the Protection of Civil Rights: Bijvoorbaatverdacht.nl.

5.4 ANPR (Automatic Number Plate Recognition)

After many years of delay (due to privacy concerns), at the end of 2018 the Dutch Senate passed another draconian law, by which the location data of millions of motorists in the Netherlands will end up in a central police database for 4 weeks, regardless of whether or not they are suspected of anything. This is the Automatic Number Plate Recognition (ANPR) Act that came into effect on January 1, 2019. Thanks in part to the financial support of countless donors, Privacy First has since been preparing a crucial lawsuit (summary proceedings and possible substantive proceedings) to suspend this law. After all, the ANPR Act constitutes a massive privacy violation and simply does not belong in a free democratic constitutional State. Privacy First has engaged the law firm CMS through Pro Bono Connect to conduct this case for us. Due to circumstances the launch of this lawsuit has unfortunately been delayed, but the preparations are now at an advanced stage and it is expected that our ANPR case will soon take place at the district court in The Hague. In this context, Privacy First has also submitted a large-scale freedom of information request to two responsible government departments.

5.5 License plate parking & right to cash/anonymous payment

Since 2014, Privacy First has been conducting legal proceedings against (mandatory) number plate parking. In the beginning of 2015, Privacy First chairman Bas Filippini won an administrative case against the municipality of Amsterdam in this regard: since then motorists throughout the Netherlands are no longer obliged to enter their registration number when parking their cars. At

the beginning of 2016, this judgment was confirmed by the Dutch Supreme Court. A new fiscal case from the chairman of Privacy First for the total abolition of number plate parking and to preserve the right to cash (anonymous) payment was unfortunately rejected by the Amsterdam district court in early 2019. This case focuses on a number of new principle questions regarding license plate parking and the right to cash payment. Privacy First expects the Supreme Court to rule on this case by mid-2020. Privacy First also hopes that this case will lead to preliminary questions about the right to cash payment at the European Court of Justice in Luxembourg. The verdict of the Amsterdam district court does not change the earlier verdicts (confirmed by the Supreme Court) that entering the registration number when parking is not mandatory.

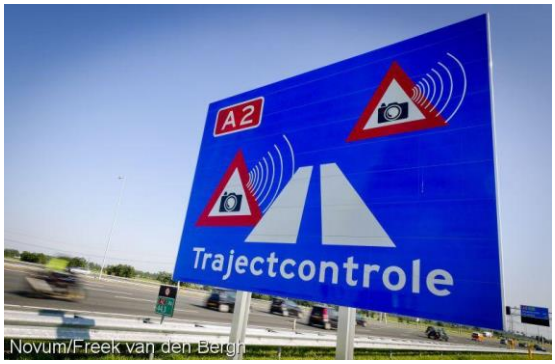
License plate parking therefore is and remains voluntary: any parking fine for not entering the license plate number must be set aside in objections and appeals, provided that the person who parked can prove that parking has been paid for.

Privacy First conducts these lawsuits to preserve and strengthen the right to anonymity in public spaces. This right has been under increasing pressure in recent years and is now in danger of becoming illusory. If necessary, Privacy First will therefore continue this case up to the European Court of Human Rights in Strasbourg.

This case is conducted at a reduced rate by Alt Kam Boer Attorneys in The Hague.

5.6 Highway section control

A similar new case from the chairman of Privacy First relates to section (speed) controls at highways: without a specific legal basis and privacy guarantees, highway section control constitutes a massive, continuous privacy violation. However, at the beginning of 2018, the Haarlem district court rejected this criminal case, followed by the Leeuwarden Appeals Court in July 2019. The Leeuwarden court refused to review the highway section control system as such against the right to privacy. During this case, however, it was revealed that all highway section control data of innocent drivers are stored for at least 72 hours and can be used for purposes other than traffic enforcement. Nevertheless, the Dutch Data Protection Authority has not intervened to date and Privacy First is forced to continue this case at the European Court of Human Rights.



This case is conducted at a reduced rate by Alt Kam Boer Attorneys in The Hague.

5.7 National Switch Point (LSP)

In recent years, the Dutch Association of Resident General Practitioners (VP Huisartsen) has conducted a large-scale civil lawsuit against the private successor to the Dutch Electronic Patient Record: National Switch Point (*Landelijk Schakelpunt*, LSP). At the end of 2017, this case was unfortunately rejected by the Dutch Supreme Court, with an important source of hope being that the Supreme Court's decision clearly points toward *privacy by design* for medical systems. It was also positive that the opinion ("conclusion") of the Advocate General at the Supreme Court made extensive reference to the *amicus curiae* letter that Privacy First and the Platform for the Protection of Civil Rights had submitted at this final appeal. This letter was submitted in the context of our joint long-term campaign SpecifiekeToestemming.nl to preserve and promote the right to medical privacy. The final appeal at the Supreme Court received pro bono support through the Public Interest Litigation Project (PILP) (partly on the advice of Privacy First) by law firm Houthoff Buruma. On the initiative of Privacy First, Houthoff subsequently continued the case before the European Court of Human Rights on behalf of several individual co-claimants (general practitioners). However, in September 2018, the European Court declared this case inadmissible without almost any explanation.

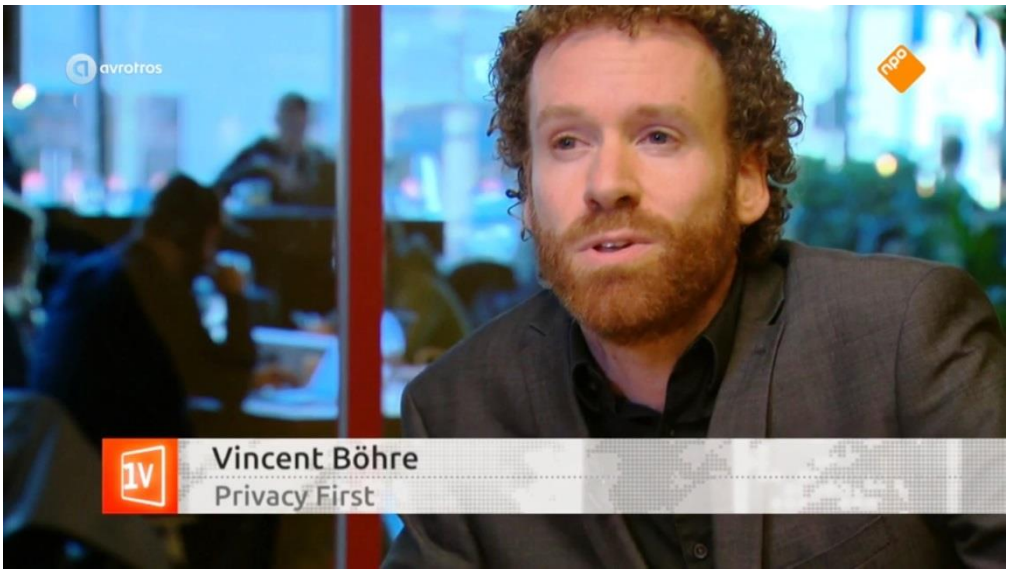
5.8 Individual court cases of privacy activist Michiel Jonker

In exceptional cases (because of our limited staffing capacity), Privacy First supports court cases of individual citizens, provided that such cases are of such a nature that our support is indispensable, in the interest of positive precedent formation, social impact, awareness and influencing legislation and policy. A good example of this are the lawsuits of Arnhem privacy activist Michiel Jonker for maintaining and promoting anonymous travel by public transport, the right to cash payment in public transport and in public places, and for the introduction of an anonymous municipal waste card with *privacy by design*. For several years, Jonker has been conducting various enforcement cases on these issues at the Dutch Data Protection Authority, the Arnhem district court and the Council of State. And with success: under pressure from Jonker's cases, the Dutch Data Protection Authority was forced by the court to investigate the "anonymous" Dutch public transport chip card and the personal waste card was declared illegal. In addition, Jonker's lawsuits often lead to inspiring media publications and critical questions at municipal and national level. Jonker conducts these cases largely on his own, without a lawyer. New cases from Jonker are in preparation and will again be supported by Privacy First.

6. Communication

6.1 Mass media

In 2018, the media reach of Privacy First grew again and became more diverse in content: on average, there was one media publication every day in 2018 in which Privacy First was mentioned or quoted, often in the press or on the internet and sometimes on radio or television. In addition to requests for interviews, Privacy First is also often approached by journalists for background information and research tips, sometimes also by foreign media.



Vincent Böhre (Privacy First) in EenVandaag, 7 March 2018. *© EenVandaag*

6.2 Internet

Privacy First's websites are our primary news and opinion channels. In addition to our Dutch-language website www.privacyfirst.nl, there is also the English-language www.privacyfirst.eu. Both sites are partly sponsored by the privacy-friendly provider Greenhost. The number of visitors to our websites grew again in 2018 and amounted to an average of 60,000 a month. Privacy First is also particularly active on Twitter and has its own LinkedIn group for privacy professionals. Both our Twitter and LinkedIn follower counts have been growing steadily for years. In addition, Privacy First is active on Facebook and will continue to offer space for (possibly anonymous) guest columns and submitted articles on our website(s). Would you like to stay informed of all developments regarding Privacy First? Then subscribe through info@privacyfirst.nl!

7. Organisation

Privacy First is an independent ANBI (Dutch Institution for General Benefit) certified foundation that largely consists of professional volunteers. In 2018, the core of our organization consisted of the following persons:

- Bas Filippini (founder and chairman)
- Vincent Böhre (director and legal advisor)
- Martijn van der Veen (Privacy First Solutions coordinator)
- Robbie van Herwerden (legal researcher)
- Simone van Dijk (theme specialist children & privacy)
- Esther Gruppen (political advisor).

The Privacy First board was expanded in the summer of 2018 and has since consisted of the following people:

- Bas Filippini (chairman)
- Paul Korremans (treasurer)
- Marc Smits (secretary)
- Ancilla van de Leest (general board member).

The Privacy First Advisory Board was established in the summer of 2018 and has since consisted of the following individuals, in their personal capacity:

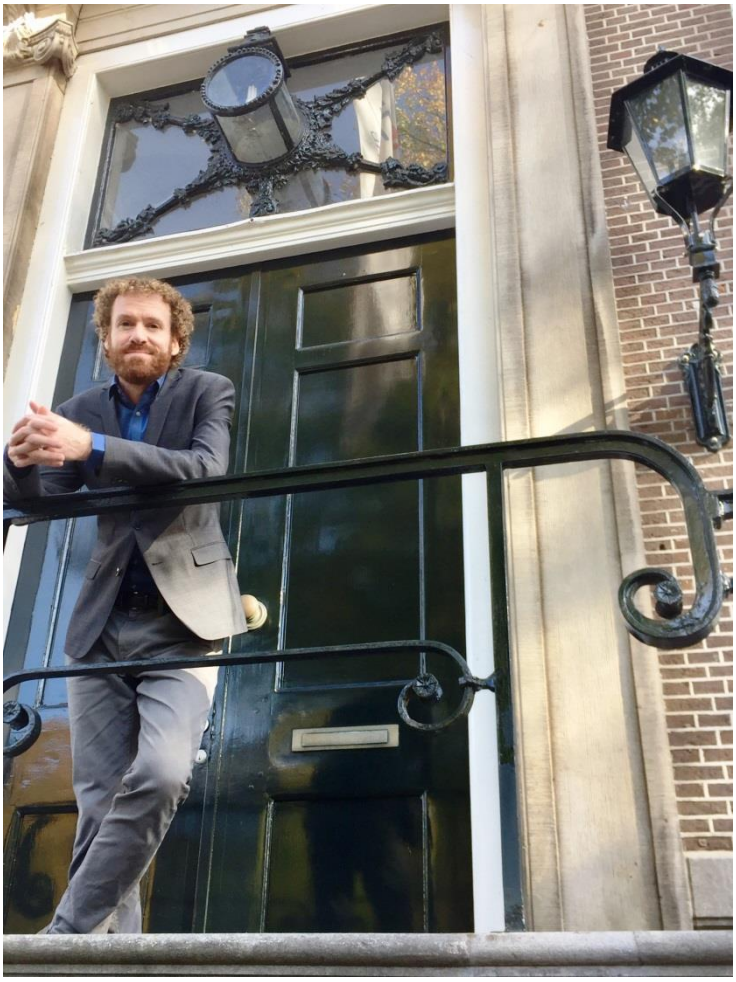
- Prof. Hans Franken (emeritus professor of Information Law, Leiden University)
- Quirine Eijkman (vice-chairman of the Netherlands Institute for Human Rights & Lector Access to Law, Hogeschool Utrecht)
- Wilmar Hendriks (privacy professional & executive coach, Control Privacy)
- Eva de Leede (senior policy officer Energy, Ministry of Economic Affairs and Climate)
- Joris Sprakel (socio-economic human rights lawyer, Fischer Group; Lecturer Human Rights Law, The Hague University of Applied Sciences).

The group of Privacy First volunteers grew again in 2018 and consists largely of professionals who support Privacy First structurally, both in content (various privacy themes and translation work) and in organisation (IT, fundraising, PR, photography) and legal research. In addition, Privacy First has an extensive network of experts from all corners of society, ranging from scientists, lawyers and IT specialists to journalists, politicians and civil servants.

At the beginning of 2019, the statutes of Privacy First were revised and updated. Privacy First has also adopted new regulations for our Advisory Board. This happened with pro bono support from the law firm Nauta Dutilh, through Pro Bono Connect.

In August 2018, Privacy First moved to a new (relatively inexpensive and well-equipped) office location on the Keizersgracht in Amsterdam. This is because our lease in the Amsterdam Volkshotel expired that summer and the Volkshotel unfortunately only wanted to accommodate tenants from the creative sector.

At the end of 2018, for its telephony Privacy First switched to privacy-friendly Voys Telecom (also corporate sponsor of Privacy First and co-plaintiff in our lawsuits against the Dragnet Act).



Vincent Böhre (Privacy First) in front of Privacy First's new office location.

8. Finances

To carry out its activities, Privacy First largely depends on individual donations and sponsorships by funds and law firms. In recent years, the number of Privacy First's donors has grown rapidly and in 2018 Privacy First's income has increased once more (30% compared to 2017). Since 2015, Privacy First receives financial support from the Democracy & Media Foundation; since 2017 this constitutes multiannual institutional support. Privacy First hopes to be able to attract other domestic and foreign funds in order to contribute to the strength and sustainability of our organization in the Netherlands and to (eventually) become operational abroad.

Apart from financial support from individual donors and funds, Privacy First welcomes corporate donations, provided that our freedom and independence are not compromised. For example, since the end of 2016, Privacy First is materially supported by Dutch IT company Detron, which distributes computers and printers to our office. Both our salary administration and our financial administration are conducted by an external administration office; the office in question offers its services as corporate sponsorship. Privacy First's websites are partly sponsored by internet services provider Greenhost and through TechSoup Netherlands our foundation can buy software at cheap prices. Kaspersky has been sponsoring our anti-virus software since 2017. Since the end of 2017, Privacy First is also supported by Voys Telecom, and since the end of 2018 Secura BV has been involved as a sponsor at the Dutch Privacy Awards. Would your company like to sponsor Privacy First too? Please get in touch with us!

It is Privacy First's standing policy to spend as much of its income on content related issues and to keep our operational costs as low as possible. For the most part, our communication (also by telephone) runs over the internet. Expensive parties and other luxuries are out of the question. Our campaigns and support activities are largely carried out by professional volunteers. Events by Privacy First are organized preferably at our own office location, or at sponsored external locations. Procedural documents in our court cases are partly self-written or supported through our own factual and legal research. It is Privacy First's established policy to enter large-scale litigation only in coalitions through the Public Interest Litigation Project (PILP) and Pro Bono Connect of the Dutch section of the International Commission of Jurists (NJCM). This is done to spread the costs and financial risks and to improve the chances of winning in court. In this way every Euro is spent as effectively as possible for the benefit of the privacy of every citizen.

Below you find our 2018 financial overview. Sponsorship of lawsuits by law firms is not included.

Annual overview	**2018**	**2017**
Revenues:		
Donations and subsidies	€ 118,741	€ 91,455
Sublease	-	€ 400
Expenditures:		
Personnel costs	€ 90,021	€ 63,137
Legal costs	-	€ 14,006

Campaign costs	€ 22,696	-
Events	€ 7,874	€ 2,340
Housing	€ 5,675	€ 4,980
Banking and insurance	€ 2,068	€ 825
Travel expenses	€ 1,813	€ 1,610
Websites	€ 1,182	€ 1,667
Communications	€ 601	€ 767
PO box and postage	€ 472	€ 431
Office costs	€ 440	€ 232
Representation expenses	€ 440	€ 758
Expense allowance scheme	€ 397	€ 454
Subscriptions	€ 266	€ 253
Miscellaneous	€ 294	€ 868

Would you like to support Privacy First? Then please donate on account number IBAN: NL95ABNA0495527521 (BIC: ABNANL2A) in the name of *Stichting Privacy First* in Amsterdam, the Netherlands, or support us anonymously through the donation page on our website. The Privacy First Foundation is recognized by the Dutch Tax and Customs Administration as an Institution for General Benefit (ANBI). Therefore your donations are tax-deductible.

Privacy First Foundation
PO Box 16799
1001 RG Amsterdam, the Netherlands
Telephone: +31-(0)20-8100279
Email: info@privacyfirst.nl
Website: www.privacyfirst.eu

Privacy First is registered in the Register of Foundations of the Amsterdam Chamber of Commerce under No. 34298157. RSIN/fiscal number: 819211710.